Kaspersky acquiert Brain4Net pour doter sa plateforme XDR d'un modèle SASE orchestré

Selon IDC, les dépenses mondiales liées au cloud dans son ensemble devraient atteindre 1 300 milliards de dollars d'ici 2025. La pandémie et son impact sur les télétravailleurs ont accéléré cette tendance et, dans ce contexte, il devient difficile pour les organisations de gérer et de protéger leurs infrastructures distribuées contre les menaces avancées. Le SD-WAN permet aux équipes de relever ce défi grâce à une gestion efficace et à une utilisation simplifiée des fonctions de sécurité pour la protection de l'ensemble de l'infrastructure.

Aller de l'avant avec une offre SASE (Secure Access Service Edge)

En raison de la généralisation du télétravail, conjuguée aux importants volumes de données et de trafic acheminés entre les services de cloud public, les succursales et les centres de données, les utilisateurs doivent impérativement bénéficier d'un accès immédiat, stable et sécurisé quel que soit leur emplacement. Ce constat a donné naissance à un nouveau concept de sécurité réseau, baptisé par Gartner Secure Access Service Edge ou SASE, qui associe sécurité et connectivité en fonction des besoins.

Grâce à l'acquisition de Brain4Net, Kaspersky entend proposer au marché une toute nouvelle offre SASE sous la forme d'une plateforme unifiée, regroupant les meilleures solutions et technologies de sécurité de Kaspersky avec les capacités et l'expertise de Brain4Net en matière d'orchestration et de contrôle des réseaux. Cette démarche stratégique permettra à Kaspersky d'offrir aussi bien des services de sécurité que de connectivité à ses entreprises clientes.

En particulier, la future offre SASE de Kaspersky intégrera à terme CASB (Cloud Access Security Broker), passerelle web sécurisée (PWS) cloud, plateforme de protection des charges de travail cloud (CWPP), gestion de la posture de sécurité du cloud (CSPM), accès réseau Zero Trust (ZTNA) et d'autres services.

Évolution du modèle XDR avancé de Kaspersky

Les solutions de sécurité existantes n'offrent pas nécessairement une approche globale de la détection et du traitement des menaces avancées. L'intégration de contrôles réseau tiers dans les solutions de classe XDR (Extended Detection and Response, détection et réponse étendue) des fournisseurs de solutions de sécurité des terminaux n'est pas suffisante pour obtenir une visibilité et des capacités d'investigation adéquates sur les incidents qui surviennent dans les environnements d'entreprise.

Cette acquisition permettra également à Kaspersky de faire évoluer ses solutions existantes vers la détection et la réponse étendue à grande échelle. Dans ce domaine, le modèle SASE présente des avantages évidents, notamment la possibilité de collecter des données télémétriques sur le trafic réseau, d'arrêter une attaque à n'importe quel endroit de la périphérie et du réseau, et

de simplifier l'orchestration et la gestion grâce à un point de contrôle unique.

La nouvelle offre XDR, basée sur une solution EDR native cloud, fournira une visibilité et des fonctionnalités avancées pour la détection basée sur IA et la logique de réponse automatique sur tous les terminaux et le réseau. En particulier, la solution XDR Kaspersky apportera un large éventail de scénarios de réponse automatisée aux incidents (blocage de l'exécution d'un fichier sur un terminal, de certains segments du réseau ou de l'infrastructure interne pour certains utilisateurs ou types d'utilisateurs) ainsi que des outils de segmentation du réseau.

En outre, elle sera basée sur une architecture de serveur unifié et permettra une gestion centralisée à partir d'une console web unique. Les clients seront en mesure de contrôler et de protéger de manière fiable tous les points d'entrée courants des menaces potentielles : réseau, trafic web, courrier électronique, postes de travail, serveurs et machines virtuelles. Ensemble, la plateforme XDR et SASE permettront aux entreprises de mettre en œuvre une stratégie Zero Trust. Outre les fonctions intégrées de détection et d'analyse technologiques avancées, la plateforme bénéficiera de renseignements de premier plan sur les menaces, constamment mis à jour et validés par les principaux experts de Kaspersky.

Un seul écosystème pour la sécurité des entreprises

Tous ces composants feront partie intégrante de l'écosystème unique qui correspond à la vision de Kaspersky pour l'avenir de la cybersécurité des entreprises. L'élément central de cet écosystème est Kaspersky Open Single Management Platform. Sur la base d'une architecture agnostique en termes de modèle de déploiement, il s'agira d'une plateforme technologique unique, native cloud, pour créer la solution XDR de Kaspersky. De cette manière, la plateforme peut être utilisée au sein d'un cloud public, d'un cloud privé ou même sur site.

« Nous sommes ravis d'unir nos forces à celles de l'équipe talentueuse de Brain4Net, qui a déjà mis au point des technologies et des services d'envergure mondiale éprouvées pour la gestion et le contrôle des réseaux. Je suis convaincu que leurs connaissances et leur expérience, combinées aux technologies de sécurité les plus primées et à l'expertise reconnue de Kaspersky en matière de gestion des menaces, s'intégreront parfaitement à notre vision de la sécurité des entreprises, tandis que les nouvelles offres aideront les responsables de la sécurité à accélérer la détection, l'investigation et le traitement des menaces, réduisant ainsi le temps moyen de réponse », déclare **Andrey Efremov, Chief Business Development Officer, Kaspersky**.

Max Kaminskiy, PDG et cofondateur de Brain4Net, ajoute : *« Nous sommes enchantés de rejoindre l'équipe de Kaspersky. La diffusion de la technologie SD-WAN nécessite un scénario commercial solide, qui correspond à la solution XDR de Kaspersky, et le choix des technologies Brain4Net confirme le haut niveau des produits et des compétences de cette entreprise. Ensemble, nous continuerons à œuvrer pour un monde plus sûr et plus confortable. »*

Pour en savoir plus sur Kaspersky Open Single Management Platform, consultez le site web.

À propos de Brain4Net

Brain4Net, Inc. propose des solutions SDN/NFV innovantes pour les grandes et moyennes entreprises et les fournisseurs de services. La plateforme B4N fournit une solution complète d'orchestration et de contrôle de réseau pour une infrastructure de réseau multifournisseur. Notre

approche aide les organisations à apporter de l'agilité au réseau, à améliorer le chaînage des services réseau et à réduire les dépenses d'investissement et d'exploitation pour le déploiement et l'exploitation de l'infrastructure réseau. www.brain4net.com

À propos de Kaspersky

Kaspersky est une société internationale de cybersécurité et de protection de la vie privée numérique fondée en 1997. L'expertise de Kaspersky en matière de « Threat Intelligence » et sécurité informatique vient constamment enrichir la création de solutions et de services de sécurité pour protéger les entreprises, les infrastructures critiques, les autorités publiques et les particuliers à travers le monde. Le large portefeuille de solutions de sécurité de Kaspersky comprend la protection avancée des terminaux ainsi que des solutions et services de sécurité dédiés afin de lutter contre les menaces digitales sophistiquées et en constante évolution. Les technologies de Kaspersky aident plus de 400 millions d'utilisateurs et 240 000 entreprises à protéger ce qui compte le plus pour eux. Pour en savoir plus : www.kaspersky.fr.